

An Insider's Guide to EDP Audits

Contributed by Vincent Leveque
Monday, 31 October 1994
Last Updated Monday, 31 October 1994

Brief: Knowing what EDP auditors can do and why they do it can help eliminate potential anxiety created by the news that you're about to be audited. Learn from an insider what you need to know to be ready for an audit.

MIS managers dread few events more than an EDP audit. Regardless of the source or intent, any audit causes stress as the auditor pokes through the labyrinth of procedures and controls. Even well-run shops rarely escape unscathed. I am familiar with this situation because I audit midrange shops for a living.

Understanding the hows and whys of an audit helps make it less painful and helps ensure that the results will come out positively.

So, what do auditors do? Auditors assess electronic data processing (EDP) procedures, controls, and security. They may review control features and overall management of the MIS function. Auditors are not strictly concerned with system security in the sense of user profiles and object authority but with the controls embedded in the entire environment.

Good auditors understand that audits are an unpleasant diversion for MIS staff, so they expect a certain amount of discomfort and defensiveness. However, auditors also have to distinguish between discomfort and evasiveness or lack of candor. Evasiveness makes it seem like you are hiding something, and small untruths about some aspects of your operation may cast doubt on any other statements you make.

However, openly discussing issues and questioning auditors about their findings is a good idea. Good auditors take the context of your overall environment into consideration, and they can help the MIS staff by suggesting creative solutions to control issues.

Types of Auditors

In many ways, the depth and nature of an auditor's review depends on who employs the auditor and the reasons for the review of MIS controls. A typical AS/400 manager may find the following types of auditors reviewing his environment:

- o Compliance auditors.
- o Internal auditors.
- o Outside public accounting firms.

Compliance auditors are most often found in government-regulated industries or industries that have substantial government business. Internal auditors are found in large enterprises. They ensure that company policies and procedures are followed and that all units of the business adhere to accepted standards of conduct and record keeping. Internal auditors may have a financial or operational focus; they may not be specialists in the specific technical details of computer systems.

Outside certified public accounting (CPA) firms conduct annual audits of financial record keeping. They may certify that financial reports are prepared in accordance with Generally Accepted Accounting Principals (GAAP). Financial audits are required by the Securities and Exchange Commission (SEC) for publicly traded companies, so all publicly traded companies are audited. Financial audits may also be required by banks and other institutions for other purposes (as a prerequisite for financing, for example).

System Controls

Although CPA firms focus primarily on financial transaction recording, they are especially interested in a specific area of computer systems: reliance. Reliance is the extent to which financial auditors can rely on information in a company's computer system without extensive manual verification. It affects the amount of work an auditor needs to do during an audit. Without reliance, financial auditors must verify manual records to ensure that transactions are entered properly and summarized accurately on the correct reports.

At first glance, reliance only seems to be an issue for the outside public accountant. However, reliance may also concern company management. It makes sense to assume that if the system is good enough to be relied upon by auditors, then company management can rely on it too. Reliance can be used as a benchmark to measure the quality of a system's controls and procedures. The quality of the information a computer system produces affects management's ability to properly manage a company and determines the true value of the computer system.

In the broadest sense, information systems are both a resource and a cost. As a resource, they must be properly secured, and as a cost, they must be effectively managed. The purpose of an EDP audit is to ensure that this important resource is properly managed and secured.

Aside from the narrow, financial perspective of reliance, controls are important in an MIS environment for the following reasons:

- o To minimize the probability of fraud or other criminal activity and to maximize detection of criminal activity.
- o To minimize the occurrence and impact of unintentional errors that affect data or systems.
- o To ensure the information systems perform as users and management believe they should.
- o To ensure the company is receiving the maximum value from its MIS expenditures.
- o To ensure proper confidentiality and access to electronic data. Like cash, information is a valued asset that must be managed and secured.
- o To ensure that hardware is properly secured and safeguarded.

The primary principle of controls is to assign responsibility. Assigned responsibility is based on the notion that specific individuals must be held accountable for the management of business resources, including MIS. It ensures that the proper individuals receive credit for a job well done. Conversely, it ensures that if assets are incorrectly or wrongly used, innocent parties are not subject to unjust blame or accusation. Many aspects of an audit, such as individually assigned passwords and date/time stamps of key records, are directly related to the need to assign responsibility for actions to specific individuals.

Audit Criteria

An audit is not primarily a technical review. Auditors focus first on the physical and procedural controls surrounding critical areas of the business. These types of controls will be described in more detail later, but briefly they involve controls over physical access to system resources and the procedures governing how these resources are managed. These controls must be effective before a company can rely on technical controls. In many cases, auditors will only look at the physical and procedural controls.

The auditor should consider the size and level of sophistication of the MIS environment. In general, a larger shop managing mission-critical systems requires a higher level of control and security than a shop with smaller, less-critical systems. An auditor may take the following into consideration.

- o The size of the MIS staff and the overall resources devoted to MIS. Larger staffs may permit and require greater controls. On the other hand, an auditor cannot require separation of functions in a shop run by one person.

- o The areas of business supported by computer systems. In general, the more a business is dependent on computers, the better controlled the systems must be.

- o The nature of the underlying business. For example, manufacturing shampoo requires different controls than manufacturing gold jewelry. Shampoo is a bulk product with a low per-unit value, while precious metals inherently require sophisticated inventory controls. These differences are reflected in the nature of the controls required in these two manufacturing environments.

- o The potential loss to the business if systems fail or are unreliable. Obviously, the more that is at risk, the tighter the control must be to reduce that risk.

- o The extent of manual controls. A review of accounts payable performed by accounting staff may offset a lack of controls embedded in the accounts payable system.

- o The degree of technical sophistication. Electronic data interchange (EDI) and other technology requires different (and sometimes stronger) controls.

The same controls are required in small shops as in larger shops. The implementation of these controls will vary depending on the size of the shop. For example, documented procedures are always required. In a small shop, these procedures may take the form of simple one-page memos on each task. A larger shop will require a more complex documentation scheme, including features such as document change management.

What Auditors Look For in MIS

The specifics of what auditors look for can be divided into three categories.

Physical: The security of the environment to intruders and potential disasters. Physical security involves use of locked doors, proper authorization to check paper stock, use of an uninterruptible power supply, and so on.

Procedural: The use of reliable, documented procedures covering all aspects of MIS.

Technical: The use of OS/400-provided features for ensuring authorized system access such as object authority, system values, and the like.

OS/400 provides many excellent features for monitoring system access, including audit journals and message queues. The system audit journal provides a wealth of information which can be accessed through a simple query. Additionally, the QUSRTOOL library provides many useful routines for security auditing.

The "Basic Audit Checklist" sidebar shows a summary of the key issues that auditors typically review. Addressing these items will help ensure that your shop receives a clean audit.

The typical audit begins with a meeting between the auditor and the MIS manager to determine the context of the MIS environment, significant issues and challenges faced by MIS, and any new developments or projects in progress. This meeting gives the auditor a sense of the complexity of the environment, which system areas may require attention, and who the auditor should talk to on the MIS staff for further information. Depending on the specific situation, the auditor may also meet with corporate management (usually the controller or vice president of finance) to gain a high-level understanding of MIS issues.

Next is usually a walk-through of the physical facilities. There is a review of the data center, work areas, and telecommunication facilities. The auditor then conducts additional interviews with the staff involved in establishing controls and security (such as local area network administrators), to gain a more detailed perspective on the control environment and the extent to which procedures are actually followed.

Documentation is reviewed to verify statements made in interviews and to ensure it is complete, up-to-date, and relevant to the existing environment. Sometimes tests of automated procedures are run, or sample reports are compared with source documents to ensure a proper match. A brief audit may take a couple of days, a more thorough one in a complex environment may take up to three weeks.

Through my experience in performing audits, I have often found certain deficiencies in AS/400 shops.

- o A lack of tested disaster recovery plans.
- o A lack of documented procedures and policies.
- o A lack of overall MIS plans.
- o A lack of control over use of the QSECOFR user ID.
- o MIS staff with inappropriate update access to production data files.

Most of these deficiencies involve areas that are not the primary mission of data processing. Understandably, most shops are busy fighting day-to-day battles to keep their systems running and to meet user requests for enhancements. Often, planning and documentation take a back seat to operating the system. However, adding documentation and controls to your day-to-day routine can help alleviate this problem.

Be Part of the Solution

Shops can reduce the annoyance level of procedural controls by making them part of routine operations. Simple forms with checklists can be helpful for repetitive tasks such as nightly backup, scheduling and execution of regular jobs, and management of user profiles.

Procedural documentation and standard forms should be maintained using appropriate software and stored on a server that is accessible to anyone who needs it. More specialized forms of automation, such as CASE tools for application documentation, and E-mail or groupware software for managing software modification requests, remove the pain from what are otherwise difficult manual documentation tasks.

Another hint for easy procedural documentation is to set up a template or outline in your favorite word processor and develop drafts of each section on an as-needed basis. The most critical documentation will be developed first, and over time you will find yourself with a remarkably complete set of procedures.

Trade-offs

At some point, it may seem counter-productive to even try to meet all of these audit objectives. The tasks required for a typical AS/400 shop to meet audit objectives can seem quite daunting. After all, shouldn't there be some balance between implementing controls and getting the rest of the work done?

EDP control issues must be viewed in the overall context of business needs. The auditor's job is to point out all the risks and vulnerabilities. However, an auditor is not (and can not be) responsible for making trade-offs between the costs of controls and their benefits. The executives of the business must make these decisions concerning controls versus expenditures. A business may legitimately accept some control risks if it feels there is a greater benefit to be had.

Alternatively, the MIS manager can work with the auditor in raising management awareness of control issues. In this case, the auditor can act as an advocate for MIS by drawing attention to the issues requiring senior management review.

The MIS manager may then be able to make the case for the budgetary resources required for important tasks such as the development of a disaster recovery plan. A smart MIS manager works with the auditors to help improve his management of the MIS environment.

Closing the Book

To summarize, proper controls help ensure that information systems are used to the benefit the business they are meant to serve. Proper controls provide more reliable and manageable systems and help enhance the prestige of the MIS function and its reputation among non-MIS management. When you have to make trade-offs between controls and other business needs, you need to keep the overall benefit to the business in mind.

Vince LeVeque currently works as a manager for KPMG Peat Marwick. Focusing on midrange systems (and specifically the IBM AS/400), his work involves system audits and other reviews of the effectiveness of information management.

Physical Controls

The computer and associated equipment must be maintained in locked room where only authorized individuals have access.

The phone closets must be locked.

The communications equipment must be in a locked facility where only authorized individuals have access.

The key must not be left in the AS/400 CPU.

The critical computer equipment must have an uninterruptible power supply (UPS) and proper climate control.

The fire and water detection equipment must be present and properly maintained.

The blank check stock (and other potentially negotiable instruments) must be properly inventoried.

The off-site storage of backup media must be in a secure, accessible location.

The printers that handle sensitive documents such as paychecks must be secure.

Dial-up access to computer systems must be controlled and monitored.

User terminals and other equipment must have proper physical access restrictions.

Procedural Controls

All procedures and policies must be documented.

There must be procedures for user profile creation and "destruction." These procedures must have a link to Human Resources for new hire, change of position, and termination.

There must be documented operations procedures for routine and emergency items.

There must be procedures for software change management, including segregation of test and production systems, as well as full user acceptance testing.

There must be documented procedures for hardware inventory and software change management.

Standard system development methodology (for shops with significant custom application development) must be used.

Formal package software evaluation and selection methodology must be used.

Project management techniques, including project definition, scheduling, and control must be used.

There must be a long-term, strategic plan that links the direction and budgets of information systems to business goals.

There must be documented standards for software coding and design, including naming conventions and good design criteria.

Security policies and procedures must be in place and documented.

Backup and restore procedures for data and programs must be in place and documented.

There must be a documented and tested disaster recovery plan.

System Controls

System value QSECURITY must be set to 30 or 40 (very important!).

Separate test and production libraries must exist. The libraries must have appropriate object authority (i.e., the programming staff must have read-only access to production data and systems).

IBM-supplied features including limited capability and object authority must be used to secure the system against unauthorized access.

Default passwords must be changed for IBM-supplied user profiles (e.g., QSECOFR, QUSER, QSYSOPR, QPGMR, QSRV, and QSRVBAS).

System values must be set to force periodic password changes, to require minimum password size, and to disable invalid password attempts (to discourage hackers). See A1 for a list of system values related to password security.

System values must be set to force periodic password changes, to require minimum password size, and to disable invalid password attempts (to discourage hackers). See Figure A1 for a list of system values related to password security.

There must be proper audit trails within transaction databases either through an explicit date/time stamping or journaling.

The QAUDJRN log must be enabled to keep a record of potential security violations. This log should be periodically

reviewed to flag unusual patterns of use. See the Setting Up Security Auditing section of the Security Reference Manual (SC41-8083, CD-ROM QBKA9H02). Also, see A1 for system values related to security auditing and check out QURSTOOL for commands that work with data from QAUDJRN.

The QAUDJRN log must be enabled to keep a record of potential security violations. This log should be periodically reviewed to flag unusual patterns of use. See the Setting Up Security Auditing section of the Security Reference Manual (SC41-8083, CD-ROM QBKA9H02). Also, see Figure A1 for system values related to security auditing and check out QURSTOOL for commands that work with data from QAUDJRN.

A1: Security-related system values

Figure A1: Security-related system values

QALWOBJRST Allow object restore option
QALWUSRDMN Allow user domain objects in libraries
QAUDCTL Auditing control
QAUDENDACN Auditing end action
QAUDFRCLVL Force auditing data
QAUDLVL Security auditing level
QCRTAUT Create default public authority
QCRTOBJAUD Create object auditing
QDSPSGNINF Sign-on display information control
QINACTITV Inactive job time-out
QINACTMSGQ Inactive job message queue
QLMTDEVSSN Limit device sessions
QLMTSECOFR Limit security officer device access
QMAXSGNACN Action to take for failed signon attempts
QMAXSIGN Maximum sign-on attempts allowed
QPWDEXPITV Password expiration interval
QPWDLMTAJC Limit adjacent digits in password
QPWDLMTCHR Limit characters in password
QPWDLMTREP Limit repeating characters in password
QPWDMAXLEN Maximum password length
QPWDMINLEN Minimum password length
QPWDPOSDIF Limit password character positions
QPWDRQDDGT Require digit in password
QPWDRQDDIF Duplicate password control
QPWDVLDPGM Password validation program
QRMTSIGN Remote sign-on control
QSECURITY System security level